Processor-based Regulatory Rule Compliant Risk Assessment & MTTHE Compliance

May 14, 2002

Professor Ted C. Giras, Ph.D.
tgiras@virginia.edu

Processor-based Rule Risk Compliant

- **ASCAP++ is Processor-based Regulatory Rule Compliant:**
  - System Hazard-free Proof-of-Correctness (Validation)
  - System Non Hazard-free Proof-of-Safety Safety Risk (Verification)
  - Operational Rule Book Compliance & Non Compliance
  - Human-factors Dispatcher, Train Crew & MOW Behavior Interactions
  - Events Passed at Danger Probabilistic Hazard Analysis (PHA)
  - Look Ahead Train Speed & Braking Profile Discrete and Continuous Simulation
  - Repair Times and Scheduled Maintenance Safety Impacts
  - Accident-pair Determined from Mishap Train Dynamic Movement Intersection
  - Risk Assessment; Societal Cost Versus Train Miles Traveled
  - MTTHE Allocation and Compliance Validation & Verification
  - Risk Containment Region High Degree of Confidence Bounds

Risk Assessment Limitations

- Risk Assessment is a Cost – Adds No New Functionality
- Not an Engineering Discipline - Knowledge and Capabilities Very Limited
- Highly Analytical – Requires Detailed System and Product Knowledge – Not Broad-based for Productivity
- Driven by Regulatory Public Policy – Not the Marketplace
- Limited Tool Sets – Validation and Verification Limited

Risk Assessment Safety Case

The Processor-based Regulatory Rule Product Safety Plan (PSP) is partitioned as:

- “*QUALITATIVE*
  - Definitions
  - Basic Principles of Safety
  - Assumptions
  - Safety Claims
  - Probabilistic Hazards Analysis (PHA)
  - Design for Safety Documentation
  - Validation and Verification Testing
- *QUANTITATIVE*
  - Hazard-free Risk Assessment
  - Train Movement PHA based on Events Passed at Danger
  - Non Hazard-free Risk Assessment
  - MTTHE Compliance
  - Risk High Degree of Confidence Bounds

Hybrid Monte Carlo Simulation Methodology

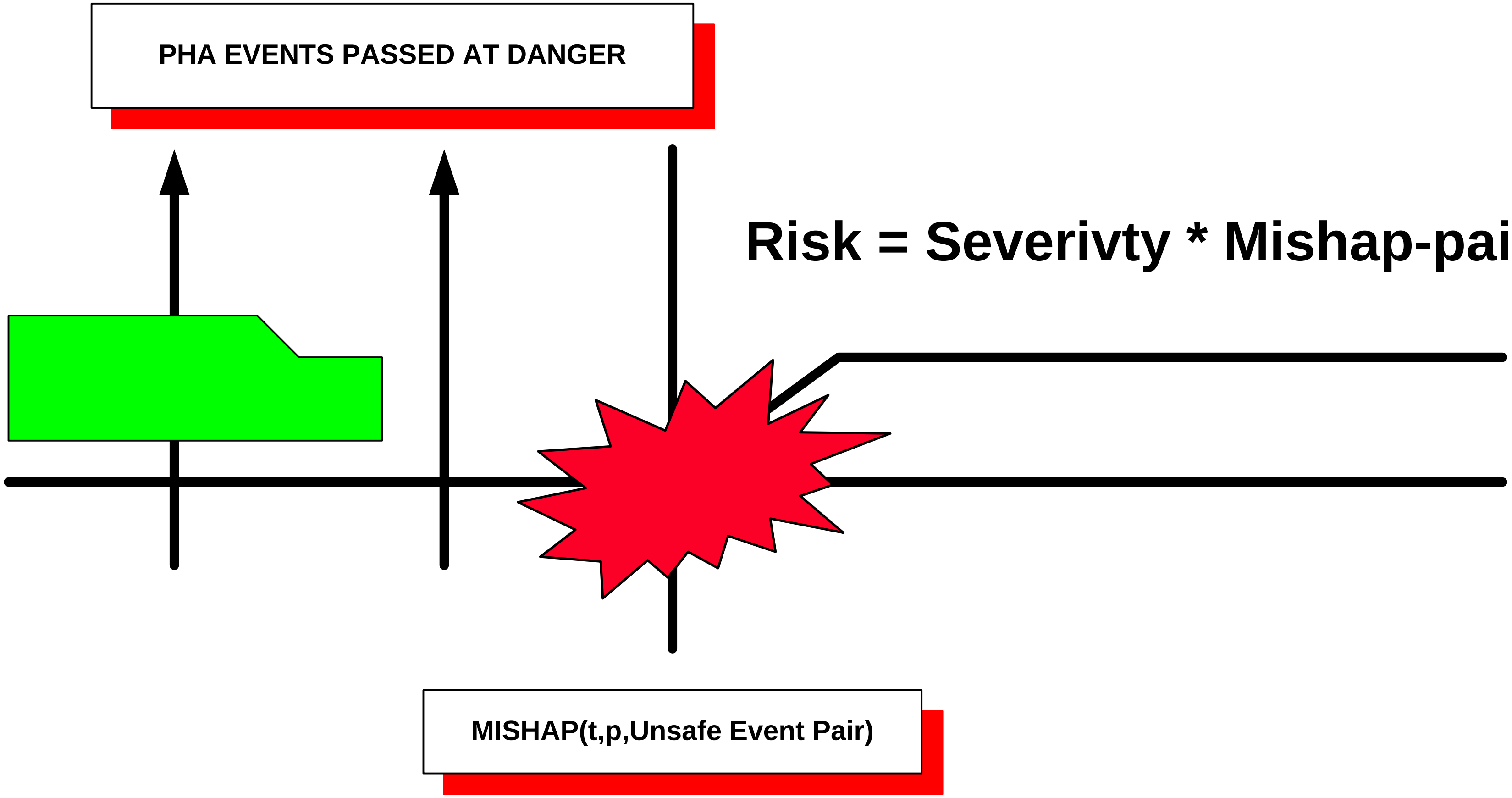
- Unified Modeling Object-oriented Compliant
  - Classes to be Presented for Industry Standard Consideration
    - ***DTC, TCS, CTC, PTC, CBTC, HGC, MAGLEV***

- Discrete Event Probabilistic Behavior
  - Stationary Objects (CAD. Wayside, Track Plan Appliances)
  - Mobile Objects (Trains, MOW Vehicles)
  - Agents (Dispatcher, Train Crews and MOW)

- Train Movement Algorithm Drives the Risk Assessment
  - Risk Exposure Determined by Train Movement Algorithm

- Continuous Look Ahead Train Dynamics
  - Precise time of Travel Estimation between Discrete Events
  - Continuous Braking Profile Train Dynamics at Mishap-pair Intersections

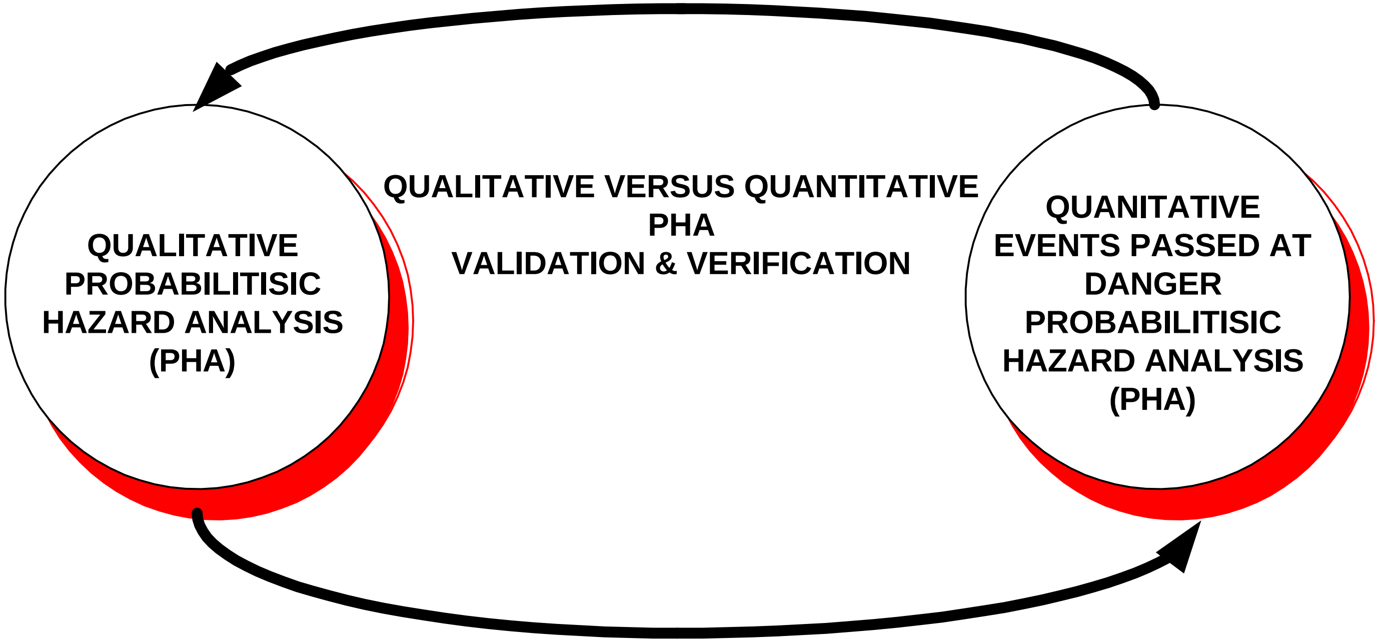
Events Passed at Danger – Mishap-pair



Risk = Severivty * Mishap-pair

Train-to-Train Mishap-pair

PHA Qualitative-Quantitative Comparison



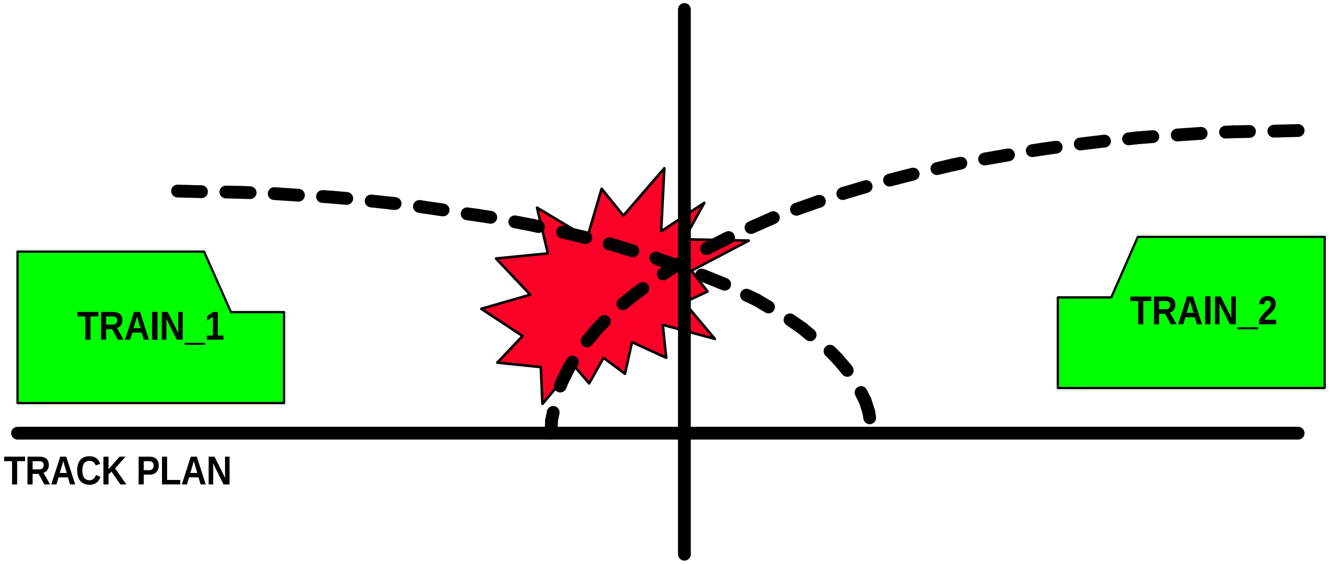
QUALITATIVE PROBABILITISIC HAZARD ANALYSIS (PHA)

QUALITATIVE VERSUS QUANTITATIVE PHA
VALIDATION & VERIFICATION

QUANITATIVE EVENTS PASSED AT DANGER PROBABILITISIC HAZARD ANALYSIS (PHA)

Mishap TRAIN-TO-TRAIN Collision-pair

TRAIN SPEED VERSUS DISTANCE -TO- GO PROFILES



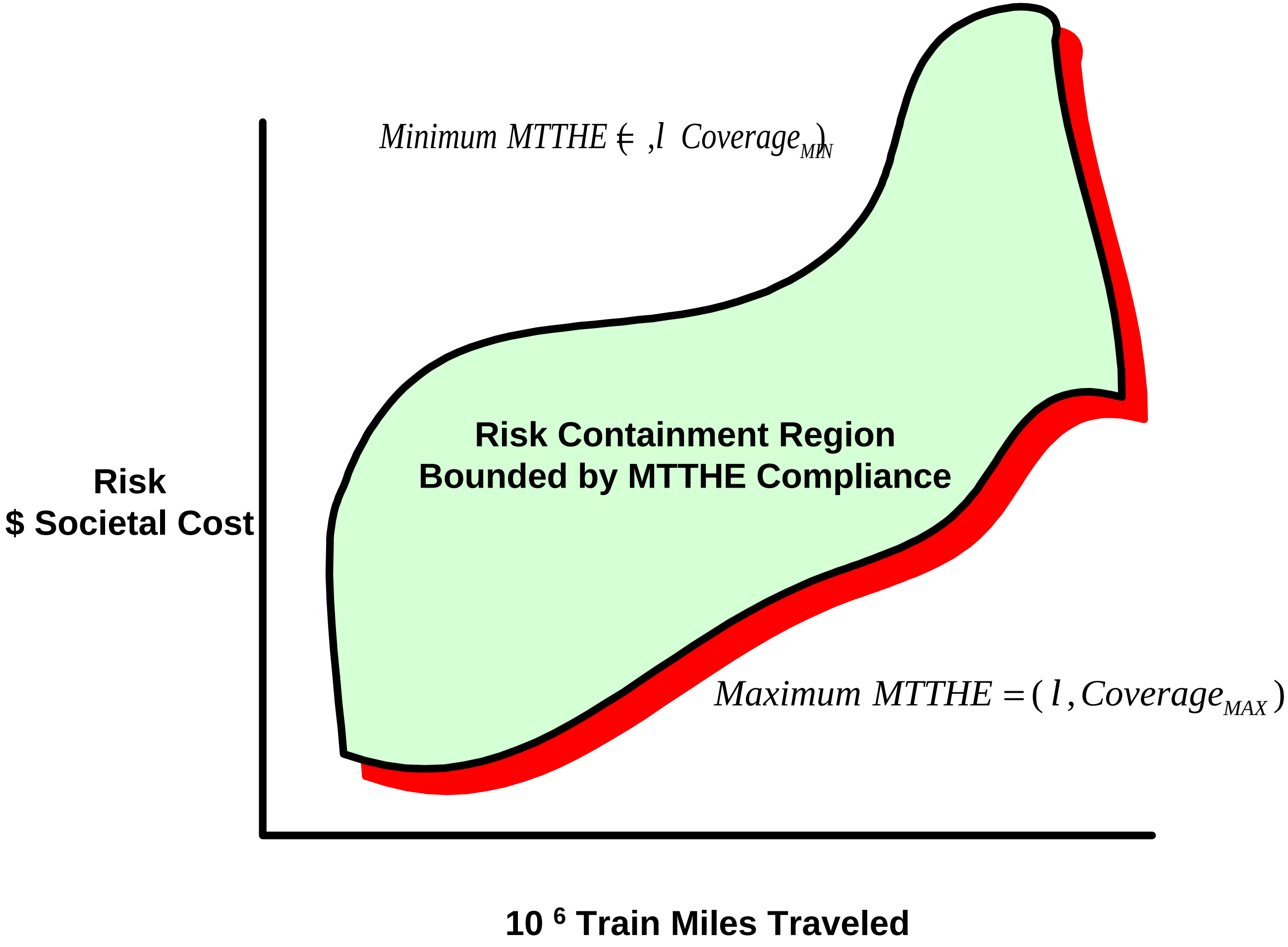
TRAIN_1 -to- TRAIN_2 MISHAP-pair

ACCIDENT SEVERITY BASED ON TRAIN CLOSING DYNAMICS

ASCAP++ Mean-Time-To-Hazard Metrics

- ASCAP++ System Hazard and Mishap Metrics:
  - Mean-Time-To-Events Passed at Danger
  - Mean-Time-To-Mishap
  - Likelihood of Occurrence of Events Passed at Danger (PHA)
  - Likelihood of Occurrence of a Mishap (PHA)
- Coverage Compliance Bounds Risk Societal Cost
  - Mean-Time-To-Hazardous Event (MTTHE) for each Processor
  - Mean-Time-To-Hazardous Event (MTTHE) for each Appliance

MTTHE Compliance Risk Confidence Bounds


Minimum MTTHE (= ,l Coverage_MIN)
Risk Containment Region
Bounded by MTTHE Compliance
Risk
$ Societal Cost
Maximum MTTHE = (l , Coverage_MAX)
10 6 Train Miles Traveled

MTTHE Ensures that Risk is Bounded